Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1997

This report was prepared by the National Counterintelligence Center.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1997	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 1997	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the National Counterintelligence Executive (ONCIX) CS5 Room 300 Washington, DC 20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**21**	

Table of Contents

Key Findings

- The *Economic Espionage Act of 1996*, signed by President Clinton on 11 October 1996, will help to protect valuable US trade secrets.[(1)]
- Updated information, as reported from the US counterintelligence community, reaffirms the findings of the 1996 *Annual Report* and includes the origin of the threat, collection targets, and methods of operation.
- Traditional threat countries and a number of non-traditional threat countries continue their collection of US trade secrets.
- The United States counterintelligence community has specifically identified the suspicious collection and acquisition activities of foreign entities from at least 23 countries.
- Analysis of updated information indicates that of those identified countries, 12 are assessed to be most actively targeting US proprietary economic information and critical technologies. This list has not changed since the 1996 *Annual Report on Foreign Economic Collection and Industrial Espionage*.
- The increasing value of trade secrets in the global and domestic marketplaces, and the corresponding spread of technology, have combined to significantly increase both the opportunities and motives for conducting economic espionage.
- Foreign collection continues to focus on US trade secrets and S&T information and products. Of particular interest to foreign collectors are dual-use technologies.
- While the clandestine efforts of foreign intelligence services continue, changes in collection methods of operation are evidenced by a transition from reliance on clandestine and illegal activity to overt and legal collection methods. This transition is not limited to commercially sponsored activity, but also includes foreign intelligence service activity.

Background

The *Intelligence Authorization Act for Fiscal Year 1995*, Section 809(b) requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the second *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 1996*, which was released in May 1996.

In coordinating a community-based response to the above requirement, the National Counterintelligence Center (NACIC) requested the assistance of the following agencies:

- Air Force Office of Special Investigations (AFOSI).
- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- Defense Investigative Service (DIS).
- Department of Commerce.

- Department of Customs.
- Department of Energy.
- Department of State.
- Federal Bureau of Investigation (FBI).
- National Security Agency (NSA).
- Naval Criminal Investigative Service (NCIS).
- US Army Intelligence and Security Command.

All of the above agencies responded to the request for information. Four agencies had no significant changes or new information to report. The remaining eight agencies provided numerous incidents and trends relating to the continuing foreign economic collection against the United States.

Structure of the Report

In accordance with the *Intelligence Authorization Act for Fiscal Year 1995*, which requires an annual update of the threat from foreign industrial espionage, Section 809(a) of the Act specifies three aspects of the threat to be reported.

In the original language from the Act:

The threat to US industry of foreign industrial espionage and any trends in that threat, including:

1. The number and identity of the foreign governments conducting foreign industrial espionage.
2. The industrial sectors and types of information and technology targeted by such espionage.

1. The methods used to conduct such espionage.

As requested by Congress, this report updates the US Government's last report on foreign economic collection and industrial espionage. Set forth is a full range of potentially damaging collection efforts against US national and corporate interests by foreign intelligence services, government agencies, private firms and other foreign entities, some of which may be sponsored at their government's national level. Their collection efforts against US economic interests and the acquisition of US technological and proprietary information may be either legal or illegal. Despite the legal nature of a large portion of foreign economic collection, much of the data sought may be sensitive in nature and may include technical, financial, and/or proprietary commercial and government information.

The Economic Espionage Act of 1996

Background

On 11 October 1996, President Clinton signed the *Economic Espionage Act of 1996*, culminating a nearly two-year effort on the part of the FBI and US industry professionals to provide new legal tools to prosecute those who are guilty of economic espionage via the theft of trade secrets. In an effort to effectively deal with the threat, the Act resolves many gaps and inadequacies in existing federal laws by specifically proscribing the various acts defined under economic espionage and addressing the US national and economic security aspects of the crime.

(2) The law also addresses the theft of trade secrets where no foreign involvement is found.

Trade Secrets

As defined in the Economic Espionage Act of 1996, the term trade secret refers to all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

- The owner thereof has taken reasonable measures to keep such information secret; and
- The information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by the public.

Before the enactment of the EEA, there was virtually no federal statute that outlawed the theft of trade secrets. Federal prosecutors were limited to using laws such as the Interstate Transportation of Stolen Property Act, the Computer Fraud and Abuse Act, and Mail and Wire Fraud statutes, to prosecute individuals for the theft of trade secrets. Due to the limitations and inadequacies of these laws in prosecuting the theft of trade secrets, it became evident that a federal statute was needed to specifically proscribe the various acts defined as economic espionage and to address the national security aspects of this crime.

Provisions

The EEA contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, instrumentality, or agent. In contrast, the second provision, under Section 1832, makes criminal the commercial theft of trade secrets, regardless of who benefits.

Reflecting the more serious nature of economic espionage, a defendant convicted for violating Section 1831 can be imprisoned for up to 15 years and fined $500,000 or both. Corporations and other organizations can be fined up to $10 million. A defendant convicted for theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined $500,000 or both. Corporations and other entities can be fined no more than $5 million. Prior to the passage of the EEA, Attorney General Janet Reno assured Congress in writing that the Department of Justice would require all prosecutions brought under the EEA be first approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Department of Justice's Criminal Division.

A defendant cannot be convicted under the EEA if it is proven that the elements of a trade secret were discovered through parallel development or reverse-engineering. In addition, the EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skills, or abilities. The EEA also does not prohibit legitimate economic collection or reporting by personnel of foreign governments by lawful means.

The EEA provides that the court, in imposing sentencing, "shall" order the forfeiture of any proceeds or property derived from violations of the EEA, and may order the forfeiture of any property used to commit or to facilitate the commission of the crime. While the EEA does not provide for civil forfeiture proceedings, it does authorize the government to file a civil action seeking injunctive relief.

Victims of trade secret thefts are often faced with the dilemma that by reporting the matter to law enforcement authorities the trade secret may be publicly revealed during criminal prosecution. In an effort to preserve the confidentiality of a trade secret, the EEA provides for the continued status of information as a trade secret and will prevent the unnecessary and harmful disclosure of such information.

The EEA should serve as a powerful deterrent and is a very important law enforcement and security management tool for protecting intellectual property rights. The EEA is not intended to convert all thefts of trade secrets into criminal cases; however, the EEA substantially raises the stakes in the arena of economic espionage.

Overview of the Threat

The development and production of trade secret information is an integral part of virtually every aspect of United States trade, commerce, and business. Hence, the security of trade secrets is essential to maintaining the health and competitiveness of critical segments of the US economy. The theft, misappropriation, wrongful receipt, transfer, and/or use of US trade secrets and other economic information, particularly by foreign governments and their agents or instrumentalities, poses a direct threat to the health and competitiveness of the US economy.

The ever-increasing value of trade secret information in the global and domestic marketplaces, and the corresponding spread of technology, have combined to significantly increase both the opportunities and motives for conducting economic espionage. As a consequence, foreign governments--through a variety of means--actively target US persons, firms, industries, and the US Government, to steal or wrongfully obtain trade secrets and other S&T information and products in order to provide their own economic and industrial sectors with a competitive advantage.

This environment presents a new set of threats to our national security and challenges existing security, intelligence, counterintelligence, and law enforcement organizations and missions.

Foreign economic and industrial interests, both government and private, also collect economic information from US firms through standard business practices such as mergers and acquisitions, strategic alliances, and licensing agreements as well as gathering publicly available information. Although these activities are an accepted element of the business world and are largely peripheral to the scope of this report, a large body of reporting indicates that these activities generate a considerable portion of the technology and economic information obtained by our competitors.

However, these activities clearly do not constitute illegal behavior.
Open-source collection activities include, but are not limited to, review of trade journals or corporate annual reports, market surveys, and attending conferences and symposia. Similarly, joint ventures and licensing agreements provide ideal opportunities to gather nonpublic information from US firms. In some instances, these types of collection efforts could be a precursor to illicit collection activities and may indicate the intelligence interest of foreign powers. At minimum, such activities and data gathered may be exploited by commercial and government analysts, research and development specialists, and officials involved with investments, acquisitions, and competitive marketplace negotiations--potentially to the disadvantage of US and private-sector interests.

Industrial Espionage and Trade Secret Theft

Technological advances are making corporate spying and theft easier and cheaper. Industrial espionage is most often carried out to gain access to corporate strategic plans, research and development information, and manufacturing process data. The power of computer technology has increased means for the theft and transfer of trade secret information. Computer age communications connectivity, commercial enterprise activities, and the posting and accessibility of corporate data on office workstations and home personal computers have made it extremely easy to copy and transfer valuable trade secret information surreptitiously. The theft of trade secrets--which encompasses all forms and types of financial, business, scientific, technical, economic and engineering information--is now a federal offense covered under the Economic Espionage Act of 1996.

Under the current counterintelligence guidance, the FBI has foreign counterintelligence responsibility in two areas directly related to economic and industrial espionage. The first area of responsibility is implementing counterintelligence programs designed to protect technologies listed on the National Critical Technologies List published by the Department of Commerce. Second, the FBI is tasked with investigating collection activities conducted by foreign intelligence services and industrial spies intended to gain access to trade secrets whose loss would undermine the strategic industrial position of the United States.
In recent years, several high-profile cases have involved foreign industrial espionage against US corporations. US companies targeted in the past have included: IBM, Corning, Inc., Honeywell Corporation, Eastman Kodak, 3M Corporation, AT&T, and General Electric. Most recently, in January 1997, under the Uniform Trade Secrets Act, General Motors won a $100 million settlement against a foreign automobile manufacturer for the activities of a General Motors executive who, in his move to the foreign firm, allegedly took with him plans for an advanced assembly line and other proprietary information.

The continued loss of trade secrets in key, high-technology industries could, over time, threaten the national security interests of the United States, and result in the loss of jobs and economic opportunity. Many US companies spend 25 to 30 percent of their budgets on research and development in hopes that they can develop products that will provide an edge in global markets.

The Cost of Economic and Industrial Espionage and Trade Secret Theft

It is difficult to assess the dollar loss as a result of economic espionage and the theft of trade secrets. The US Intelligence Community has not systematically evaluated the costs. The extent of the economic intelligence operations targeting US industries is especially difficult to ascertain. United States industry is reticent about publicly acknowledging

cases of possible breaches of corporate security by their own employees, foreign intelligence services, or foreign competitor organizations. Nonetheless, recent studies by the US private sector estimate that the loss to businesses from theft and misappropriation of proprietary information runs in the billions of dollars each year. In particular, in its March 1996 study, The American Society for Industrial Security estimated that the potential losses from foreign and domestic trade secret theft for all American industry could amount to $2 billion a month.

Origin of the Threat

The FBI and other members of the counterintelligence community have reported that foreign intelligence activities directed at US critical technologies pose a significant threat to US national security. According to these agencies, even certain US allies are actively attempting to obtain US information through unauthorized means. During the past year, the US counterintelligence community has specifically identified the suspicious collection and acquisition activities of foreign entities from at least 23 countries. Of these, 12 have been identified as the countries most actively targeting trade secret information.

(3) These countries are assessed to be the most aggressive in collection efforts directed against US proprietary economic information and critical technologies. In addition to overt and legal information-gathering activities, these countries are willing to employ clandestine and illegal methods to collect against US interests.
The number and identity of the 12 countries assessed by NACIC to be most actively targeting US information has not changed since the 1996 *Annual Report*, and as indicated last year, has increased only slightly from 10 to 12 countries since the 1995 *Annual Report*. It should be noted that the current list of 12 countries does not reflect the full picture of targeting against US economic interests--only the most serious threat.

Counterintelligence community updates reaffirmed the 1996 *Annual Report* findings. Reporting agencies cited a substantial amount of suspicious activity potentially involving economic and industrial espionage and/or intelligence collection. It is important to note that preliminary identification of a foreign entity does not prove knowledge or sponsorship by the government of that country. Despite this fact, the number and frequency of these cases, as seen below, reflects the need for greater attention.

Based on US defense industry reporting of suspicious activity, the Defense Investigative Service (DIS) has continued to observe trends of low-level collection interest and activity by foreign companies and governments. Traditional threat countries continued their collection activities. The counterintelligence community also observed continued collection by nontraditional threat countries. According to DIS, as the frequency and

numbers of suspicious reports from cleared contractors continued to grow in 1996, the number of different countries involved in some form of suspicious contact also grew. Although the numbers of reported incidents and countries increased in 1996 over that reported by DIS in 1995, these incidents have been referred to the appropriate Intelligence Community agencies for investigation and analysis. Outcomes of these investigations remain pending and no conclusive judgments are possible at this time.

Targeted Information and Technology

Foreign collection continues to focus on US proprietary economic and technical information and products. Further, programs associated with dual-use technologies, those that can be used for both military and civilian applications, are consistent targets for both foreign government and foreign commercially sponsored collection activity.

A 1996 DIS summary of foreign contacts indicated that numerous foreign countries displayed some type of suspicious interest in one or more of the 18 technology categories listed in the Military Critical Technology List (MCTL), which is published by the Department of Defense. These major technology categories include:

- Aeronautics systems.
- Armaments and energetic materials.
- Chemical and biological systems.
- Directed and kinetic energy systems.
- Electronics.
- Ground systems.
- Guidance, navigation, and vehicle control.
- Information systems.
- Information warfare.
- Manufacturing and fabrication.
- Marine systems.
- Materials
- Nuclear systems.
- Power systems.
- Sensors and lasers.
- Signature control.
- Space systems.
- Weapons effects and countermeasures.

The majority of the technologies included in the MCTL are dual use. As a result, the loss or compromise of proprietary or embargoed information concerning these technologies can affect both the economic and national security of the United States.

According to the Department of Energy (DOE), foreign researchers have gained fully sanctioned access to numerous sensitive technologies during preapproved visits and assignments to DOE facilities. (4) According to the most recent DOE information, approximately 50,000 foreigners visited DOE facilities during 1994 and 1995. Such a volume of visitors, although legal and officially arranged, can present significant security concerns if sound risk management is not practiced. The pursuit of access to a particular program, technology, or US specialist by visiting researchers may be an espionage precursor.

DOE information indicates that the most frequently accessed sensitive technologies in 1994 and 1995 were ceramics, cermets, (5) and refractories, (6) which were accessed 148 times in 1994, and 155 times in 1995. DOE has specifically identified six additional sensitive technologies that have been accessed by foreign countries believed to engage in economic collection. These technologies are advanced automotive propulsion, composite materials, nuclear radiation sources, safeguards, superconductivity, and uranium enrichment.

The most frequently accessed "nonsensitive technologies" by foreign visitors and assignees to DOE facilities were environmental sciences-terrestrial in 1994, and biomedical sciences-basic studies in 1995.

According to DOE's most recent statistics, the four DOE facilities that host the most foreign visitors and assignees are Oak Ridge National Laboratory, Lawrence Livermore National Laboratory, Argonne National Laboratory-East, and Pacific Northwest Laboratory.

In addition, counterintelligence community reporting continues to reflect increasing trends of foreign collection activity involving proprietary strategic management information, to include bid proposals, price structuring, trade developments, marketing plans, and proposed US legislation affecting foreign firms operating in the United States.

Computer Crimes

In addition to trade secrets obtained from employees or company documents and publications, US Government and private-sector computer networks present an increasingly attractive target for illicit activities. Computer intruders can move freely without reference to state borders and can perform their tasks without gaining physical access to the system under attack. These factors make it more difficult to detect the theft of information and the origin of the intruder. Aside from stealing information, a computer intruder can also introduce a "virus" into a competitor's computer system to sabotage its operations.

According to a study conducted by the Computer Security Institute (CSI), a San Francisco-based association of information security professionals, computer crimes are soaring, and companies should be on the alert for security breaches. The *1997 Computer Crime and Security Survey* was conducted by CSI in cooperation with the FBI's International Computer Crime Squad in San Francisco. Both CSI and the FBI stated that the results of this survey will be used to better understand the threat of computer crime and provide law enforcement with some basic information with which to address the problem more effectively.

According to the survey, about 75 percent of the 563 responding corporations, government agencies, financial institutions and universities surveyed by CSI reported financial losses in the past 12 months. Last year financial losses from financial fraud, computer viruses, sabotage, and theft of proprietary information and laptops were up seven percent and topped $100 million. Reflecting the increased competition in the global marketplace, over 50 percent of the respondents cited foreign competitors as a likely source of attack and 22 percent cited foreign governments as a likely source of attack.

The survey also showed that only 17 percent of the respondents reported crimes to law enforcement authorities. There appears to be reluctance on the part of the private sector to report allegations of computer and economic crime to law enforcement authorities. A large number of these crimes go unreported because of a company's fear of undermining the confidence of their shareholders, negative publicity, and further exposure of trade secret information during prosecution.

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, employs International Computer Crime Squads in selected offices throughout the United States. These squads investigate violations of the Computer Fraud and Abuse Act of 1986, including major computer network intrusions, privacy violations, industrial espionage, pirated computer software, and other crimes where the computer is a major factor in committing the criminal offense.

As a result of its 1994 Economic Counterintelligence Program, the FBI has developed a growing volume of information on foreign economic threats including the identification of those countries who pose these threats, their targets, and the methods they use. In response to the increase in computer crimes, the FBI established a Computer Investigations and Infrastructure Threat Assessment Center (CITAC) to provide analysis and support to all levels of the criminal justice system.
The Department of Defense (DOD) has received substantial Congressional funding for program initiatives in 1996 and 1997 to create a DOD Computer Investigations Training Facility (DODCITF) and a DOD Computer Forensics Laboratory (DODCFL). The DODCITF and the DODCFL will address the increasing risk of computer-based threats to defense technologies and military readiness. These DOD initiatives respond to the exponential growth in DOD's reliance on computer networks and the increased risks

posed by computer intrusions; the growing number of computer-related incidents and investigations within the DOD; and the increasing volume of computer evidence collected and analyzed by DOD investigative organizations.

Because of the growing use of the Internet for commercial and financial transactions, more opportunities will be available for the computer intruder. While no security system is guaranteed to provide absolute protection, additional efforts in the area of information security could prevent substantial losses.

Collection Methods

Practitioners of economic and industrial espionage seldom use one method of collection; rather, they combine a number of collection techniques into a concerted collection effort that combines legal and illegal, traditional, and more innovative methods.

Espionage and Other Illegal Collection Methods

Traditional clandestine espionage methods, such as agent recruitment, US volunteers and co-optees, surreptitious entry, theft, SIGINT intercept, computer penetration, and other specialized technical operations continue to be used by foreign intelligence services targeting US interests.

Lawful Collection Methods

In addition to traditional espionage and other illegal activities, foreign governments, instrumentalities, and agents gather economic intelligence via numerous other methods. These methods involve legitimate practices that do not constitute illicit activity. While foreign governments and their entities have been known to turn legitimate transactions and business relationships into clandestine collection opportunities, often the overt collection of economic information is practiced for legitimate purposes. Although some of these legal activities may be a precursor to clandestine or illegal collection, they do not of themselves constitute evidence of illegal activity.

While most industry associations with foreign entities are in fact economically advantageous to the United States, a DIS summary of 1996 suspicious contacts that were reported by defense contractors, indicated that foreign entities employ a variety of

legitimate collection methods in attempting to acquire US proprietary economic information. Despite the legitimate nature of these collection practices, they may be an important element in a broader, directed intelligence-collection effort. Last, the legitimate collection of economic information, in addition to clandestine methods that constitute economic espionage, depict the broad scope of a successful foreign economic intelligence-collection program.

Defense industry reporting continues to reflect increasing trends of foreign collection activity. As reported by DIS, foreign intelligence services and foreign private industries, which may or may not be sponsored by a foreign government, employ the following legal collection methods.

Unsolicited Requests for Information

According to DIS, the most frequently reported method of operation (MO) used by foreign entities is the unsolicited request for information. This method is simple, low cost, nonthreatening and low risk. The unsolicited request for information is a popular MO of countries against which the United States has imposed an embargo and of foreign entities who may attempt to disguise the end user through the use of front companies. A reported majority of suspicious unsolicited requests for information involved data covered under the International Traffic in Arms Regulations (ITAR) that could not be lawfully exported without a license.

A growing number of incidents involve mail, fax, phone, and Internet requests from a foreign entity to a cleared contractor. The Internet provides a direct line of communication for foreign-collection efforts. Internet access to a company's bulletin board, home page, and employees, provides foreign collectors with many avenues through which they can broaden their collection efforts.

Foreign collectors have also employed the use of marketing surveys to solicit information that often exceeds generally accepted terms. Surveys may solicit proprietary information concerning corporate affiliations, market projections, pricing policies, purchasing practices, and types and amounts of US Government contracts.

Inappropriate Conduct During Visits

Inappropriate conduct during visits was the secondmost frequently reported MO associated with foreign-collection activity. Once in a facility, collectors may attempt to manipulate the visit to satisfy their collection requirements. For example, visitors may ask questions or request information that is outside the scope of the approved visit.

Unchecked, this MO usually results in the loss of technology, and is therefore considered to be a damaging form of collection activity.

Solicitation and Marketing Services

Foreign individuals with technical backgrounds may be solicited by, or may themselves seek to, market their services to research facilities, academic institutions, and even cleared defense contractors. This method of collection was reported to the DIS with greater frequency during the past year. In addition, US technical experts may be requested by foreign entities to visit a foreign country and share their technical expertise. Usually associated with alleged employment opportunities, there is also an increasing trend involving "headhunters" who solicit information from targeted employees. In these instances, such solicitation may be a ploy to access and gather desired information.

International Exhibits, Conventions, and Seminars

International exhibits, conventions, and seminars are rich targeting opportunities for foreign collectors. These functions directly link programs and technologies to knowledgeable personnel. At these venues, foreign collectors target US scientists and businessmen to gain insights into US products and capabilities. Consequently, US defense industry reporting indicates that collection activity at these events is usually expected, is commonplace, and most often involves overt open-source intelligence gathering.

The counterintelligence community has increasingly sought to make the private sector aware of the foreign collection threat and has conducted threat awareness briefings prior to such international symposia. Specific examples include counterintelligence and security awareness briefings for US industry representatives who planned to attend or support the Paris and Farnborough International Air Shows.

Joint Ventures and Front Companies

Joint ventures, joint research, and exchange agreements potentially offer significant collection opportunities for foreign entities. As with other MOs, joint efforts place foreign personnel in close proximity to US personnel and afford potential access to S&T programs and information. Through joint-venture negotiations, US contractors may

reveal unnecessarily large amounts of technical data as part of the bidding process. In addition, a number of governments use front companies to gather intelligence and provide cover for intelligence operations.

Acquisition of Technology and Companies

Despite the existence of the Committee on Foreign Investments in the United States (CFIUS), foreign acquisition of technology and companies in the US defense industry continues to generate significant concerns regarding foreign access to US markets and sensitive proprietary information. CFIUS reviews foreign mergers and acquisitions of US firms to determine the impact on US national security and provides guidance on arrangements with foreign governments for advance consultations on prospective major foreign governmental investments in the United States. However, while it is beneficial for a foreign entity to notify CFIUS of its intent to purchase or merge with a US company that holds classified DOD contracts, it is not mandatory. Foreign investors in a US private-sector company need not notify CFIUS of their intentions.

Co-Opting of Former Employees and Cultural Commonalties

Incidents involving the co-opting of former employees who had access to sensitive proprietary or classified S&T information remains a potential counterintelligence concern. Frequently, foreign collectors will exploit cultural commonalties to establish rapport with their target. As a result, foreign collectors specifically target foreign employees working for US companies. Likewise, US defense contractor employees working overseas may be particularly vulnerable to foreign offers of employment as their contracts expire.

Open-Source Collection

The openness of the American society and the wealth of technical, scientific, political, and economic information available through the open media provide US adversaries with a vast amount of detailed, accurate, and timely information. The use of open-source information as an intelligence source has a number of benefits. It is relatively cheap to obtain, it is legal in the majority of instances, and it makes up the greatest volume of information accessible to an intelligence collector. Because of these benefits, open-source

information has increasingly been exploited by many foreign entities, to include foreign intelligence services in an attempt to target the United States.

The global growth of the Internet has changed the accessibility and ease with which foreign collectors can gather data. Reporting indicates that foreign collectors have increased their direct connections with Internet service providers. Information available through electronic databases continues to expand as the number of databases and electronic bulletin board systems available to the public continues to grow dramatically. Bulletin board systems, some of which track sensitive US Government activities or provide information on proprietary activities performed by government contractors, have grown rapidly on the Internet.

Appendix

ECONOMIC ESPIONAGE ACT of 1996

Title 18 U.S.C. 1831 et. seq.
Sec. 1831 Economic Espionage
(a) In General.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

1. steals, or without authorization appropriates, takes, carries way or conceals, or by fraud, artifice, or deception obtain a trade secret;
2. without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
3. receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization;
4. attempts to commit any offense described in any of paragraphs (1) through (3); or
5. conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations. Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Sec. 1832 Theft of Trade Secrets
(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly --

1. steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtain such information;
2. without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
3. receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained or converted without authorization;
4. attempts to commit any offense described in paragraphs (1) through (3); or
5. conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

Sec. 1833 Exceptions to prohibitions
This chapter does not prohibit --

1. any otherwise lawful activity conducted by a governmental entity of the United States, a State, or political subdivision of a State; or
2. the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

Sec. 1834 Criminal Forfeiture
(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States --

1. any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
2. any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject of forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by Section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section which shall not apply for forfeitures under this section.

Sec. 1835 Orders to Preserve Confidentiality
In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the

confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedures, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

Sec. 1836 Civil Proceedings to Enjoin Violations
(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.
(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

Sec. 1837 Applicability to Conduct Outside the United States
This chapter also applies to conduct occurring outside the United States if --

1. the offender is a natural person who is a citizen or permanent resident alien, or organization organized under the laws of the United States or a State or political subdivision thereof; or
2. an act in furtherance of offense was committed in the United States.

Sec. 1838 Construction with Other Laws
This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under Section 552 of Title 5 (commonly known as the Freedom of Information Act).

Sec. 1839 Definitions:
As used in this chapter--

1. the term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;
2. the term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;
3. the term "trade secret" means all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

    (a) the owner thereof has taken reasonable measures to keep such information secret; and

(b) the information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by, the public; and

1. the term "owner," with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

CLERICAL AMENDMENT--The table of chapters at the beginning part 1 of Title 18, United States Code, is amended by inserting after the item relating to Chapter 89 the following:
90. Protection of trade secrets .....1831.

REPORTS--Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by Section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601).

Footnotes

(1) The definition of the term "trade secret" in the Economic Espionage Act is very broad and generally includes all types of information, however stored or maintained, which the owner has taken reasonable measures to keep secret and which has independent economic value.
(2) The *Economic Espionage Act of 1996* and its provisions are further discussed in detail under a separate heading. A reproduction of the Act can be found in the appendix of this report.
(3) This version of the report does not identify the specific countries. Each CI agency provided NACIC with compilations of incidents and trends that appeared to involve the targeting of US economic and industrial information during the past year. NACIC, as coordinator, compiled a master list of countries assessed to be the most aggressive collectors of US information. Due to each CI agency's differing mission, investigative responsibilities, and reporting criteria, one agency's list of foreign collectors could differ from that of another. NACIC's analytic effort in compiling a master list sought to ensure the integrity of submitted data and consistency with the assessment criteria used in its initial 1995 *Annual Report*.
(4) A sensitive technology is an unclassified subject/topic identified by DOE that involves information, activities, and/or technologies that are relevant to national security. Disclosure of sensitive subjects has the potential for enhancing foreign nuclear weapons capabilities, divulging military critical technologies, or revealing other advanced technologies.
(5) A heat-resistant, bonded mixture of ceramic material and a metal used in gas turbines, nuclear reactor mechanisms, and rocket motors, and so forth.

(6) Heat-resistant, hard to melt substances such as ores and metals.